RESPONDING TO A DATA BREACH

SECTOR 2017

Iain Paterson, Managing Director
PRESENTATION OVERVIEW

Pre-Breach
- Incident Response Planning
- Know yourself better than a hacker does
- Being Prepared
- Being Protected

During a Breach
- Detecting a Breach
- Resources and Teams
- Analysis and Coordination
- Business Impact
- Communication Strategy
- Containing and Triage
- Evidence and Forensics
- Business Recovery

Post Breach
- Lessons learned and closing gaps
- Preparing for the next one
- Retaining evidence
- More communication and coordination

“Well, in our country,” said Alice, still panting a little, “you'd generally get to somewhere else—if you run very fast for a long time, as we've been doing.”

“A slow sort of country!” said the Queen. “Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!” – Lewis Carroll
PRE-BREACH PREPARDNESS
# INCIDENT RESPONSE PLANS AND CONSIDERATIONS

## An Incident Response Plan Should Define

- Roles and responsibilities
- Incident handling strategy
- Command and control structure
- Metrics for effectiveness of plan

## Tools and Capabilities

- What do you have?
- What are the gaps in your capabilities?

## Notification Plan

- Legal review - Regulations and Compliance by Industry/Jurisdiction

## Budget Inclusion
KNOWING YOUR ENVIRONMENT

- UP TO DATE ASSEST INVENTORY
  - Knowledge base of system configurations (build books)

- NETWORK AND DATA FLOW DIAGRAMS
  - Physical and logical

- LOGGING AND DETECTIVE CONTROLS
  - Sufficient logging and retention
  - Keep your logs secured
BEING PREPARED

BACKUPS

• Current and tested
• Backups secured
• Backup infrastructure secured
• Commonly attacked during a breach

AWARENESS AND TRAINING

• What do you have? Phishing still the number one vector for data breaches
• Run drills and simulations
• Train not just technical people, but also business leaders
BEING PROTECTED

RISK ASSESSMENTS

• Penetration Testing
• Security Assessments and Audits
• VA (Vulnerability Assessment) Program

OTHER TOOLS

• Incident Response and Forensic Tools
• IDS / IPS
• Malware Tools
• “Blinking Boxes”
RESPONDING TO A BREACH
DETECTING A BREACH

IDENTIFYING A BREACH HAS ACTUALLY OCCURRED

Best - Sec Ops team + Controls = Instant Detection

Common - Sys Admin or User + Weird Behaviour = 200 Days+

Bad - Law Enforcement Phone Call

Worst - "Hi this is Brian Krebs, would you care to comment...."
# MOBILIZING YOUR RESOURCES

## ORGANIZING RESOURCES AND TEAMS
- A Central IR team or Incident Handler needs to take the lead role
- Secondary coordination roles may be necessary depending on scale of incident and geography of resources

## 24/7 PROBLEM
- 12 hour shifts

## BRING RESOURCES IN BASED ON THE NECESSARY SKILLSETS TO COMPLETE THE TASKS AND ANALYSIS REQUIRED
- Incident Handler or Senior Management makes the call
- Manage the size of the incident response closely
# ANALYZING THE INCIDENT

## WHAT’S NORMAL VS. WHAT’S HAPPENING

- What’s changed recently
- Network traffic anomalies
- Bring in help if you can’t handle it internally

## DOCUMENT *EVERYTHING* DURING THIS STAGE – IT MAY BE HIGHLY RELEVANT LATER!

- 12 hour shifts
- Current Status, Previous Status
- Summary of events
- Indicators of event / breach
- Actions taken and remediation effort status
- Evidence and Chain of Custody - Forensically sound process
- Next steps in response
INCIDENT CLASSIFICATION AND COMMUNICATION

CLASSIFY THE INCIDENT AND THE IMPACT

- How is my business impacted?
- Am I obligated to disclose
- What is the nature of the impact (Privacy, Availability, Integrity, Multi-Dimensional)?

SOME EXAMPLES OF INCIDENTS (MALWARE, RANSOMWARE, INSIDER FRAUD, INSIDER MALICIOUS, TARGETED PHISHING/WHALING)

NOTIFYING ORGANIZATIONS AND STAKEHOLDERS

- Senior Management
- HR, Finance, other business units
- Controlling the message so as not to spread panic
- Limited Distribution
EXTERNAL COMMUNICATION PROCESSES

COMMUNICATION AND COORDINATION

- Legal Team as a Funnel
  - Media Communication Strategy
    - Single Point of Contact (Media Training)
    - Have Prepared statements ready
    - Explicitly remind all staff NOT to go outside these channels

- Law Enforcement
  - Centralize this communication through one person (likely legal)

- Have one person on the IR team who works with LE

- Public Safety
  - CCIRC (Canadian Cyber Incident Response Centre)
### WHAT TO PRIORITIZE

- Minimize the spread of damage or breach
- Preserve Evidence
- Keep business critical services available as much as possible (assuming they are not compromised)
- Timelines and effort for remediation

**These are strategies that can be run individually or in parallel depending on organizational goals**

### HOW TO CONTAIN

- Isolate devices from the network
- Create VLANS or Sandboxes
- Firewall rules and IPS signatures
- Antivirus Signatures
- System Inventory tools or other mechanisms to scour for IOCs
- Multiple Teams focused on different efforts to reduce time
EVIDENCE GATHERING AND FORENSICS

To Assist LE and Future Legal Proceedings (including defense)

Retain Relevant Logs and Data
- Identifying affected systems and data
- Mechanisms to search (Splunk, Hadoop, etc)
- SIEM

When to call the experts
- Chain of Custody
- Laws and Regulations that may apply
RECOVERY

Largely safer to rebuild from scratch and recover data

Fix and verify the root cause issue

Patch everything as soon as possible

High Value Systems / Business Critical prioritized

Update your inventory and build books during this phase
POST BREACH BEHAVIOUR
## GETTING THINGS BACK ON TRACK

<table>
<thead>
<tr>
<th>WHAT WENT RIGHT? WHAT WENT WRONG?</th>
<th>RETENTION OF EVIDENCE</th>
<th>TESTING YOUR DEFENSES</th>
<th>COMMUNICATION AND COORDINATION AGAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>What resources were used effectively?</td>
<td>3 years recommended</td>
<td>Pen-Testing</td>
<td></td>
</tr>
<tr>
<td>What tools or capabilities did we not have?</td>
<td>Factor in costs of storage, loss of hardware</td>
<td>Phishing Exercises</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ongoing security program w/ milestones</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notification to clients and business partners of the outcomes</td>
<td></td>
</tr>
</tbody>
</table>